Mission-focused Cyber Security and the Cyber-Next Concept

AMC/A6OS
DSN 779-6298

Mission-focused Cyber Security

- **The newly created Defensive Cyberspace Operations (DCO) Implementation Guidance provides detailed information on the purpose, intent and way ahead for initial implementation of Communications Squadron-Next (CS-N) and, specifically, MDT across pathfinder units around the Air Force.**
- **The (CS-N) Pathfinders and Mission Defense Teams (MDT) are programs designed to organize, train and equip cyber forces to battle in a degraded or operationally-limited environment.**
- **It is vital that the CS-N and MDT focus on building capabilities to secure and defend AF mission systems operating within the Air Force Information Network, against current and future threats around the globe within a broader warfighting context. .**
- **US forces can no longer operate with impunity in the cyber domain because of threats from state and non-state actors.**

SAF/CIO Lt. Gen. William J. Bender envisions Initial Operating Capability between May 2017 and Sept 2017.

DCO Implementation Guidance

- **DCO Implementation Guidance:**
  - **Proposes a new employment type for Airmen of the Communications Squadron-Next (CS-N) series of pathfinders and introduces the concept of *persistent* enclave defense.**
  - **Provides background and history of the Air Force's experience with assembling and fielding Cyber Protection Teams (CPT) to the Cyber Mission Force (CMF).**
  - **Discusses challenges and proposals on how to link CS-N teams to other initiatives in Air Force cyberspace defense.**
  - **Repurposes Airmen to transition from traditional Information Technology (IT) enterprise service delivery to an acknowledgement that all Air Force weapon, mission and support systems rely upon (or exist within) a cyberspace domain that is contested by Advanced Persistent Threat actors (APT).**
  - **Evolved over a number of years as the Air Force sought to balance the demands of decreasing budgets against the exponential increase in cyberspace attacks against core infrastructure and weapon/mission systems.**

SAF/CIO A6 Vision:
The Air Force fully exploits the man-made domain of cyberspace to execute, enhance and support Air Force core missions.

Unrivaled Global Reach for America … ALWAYS!

Cyber-Next Concept

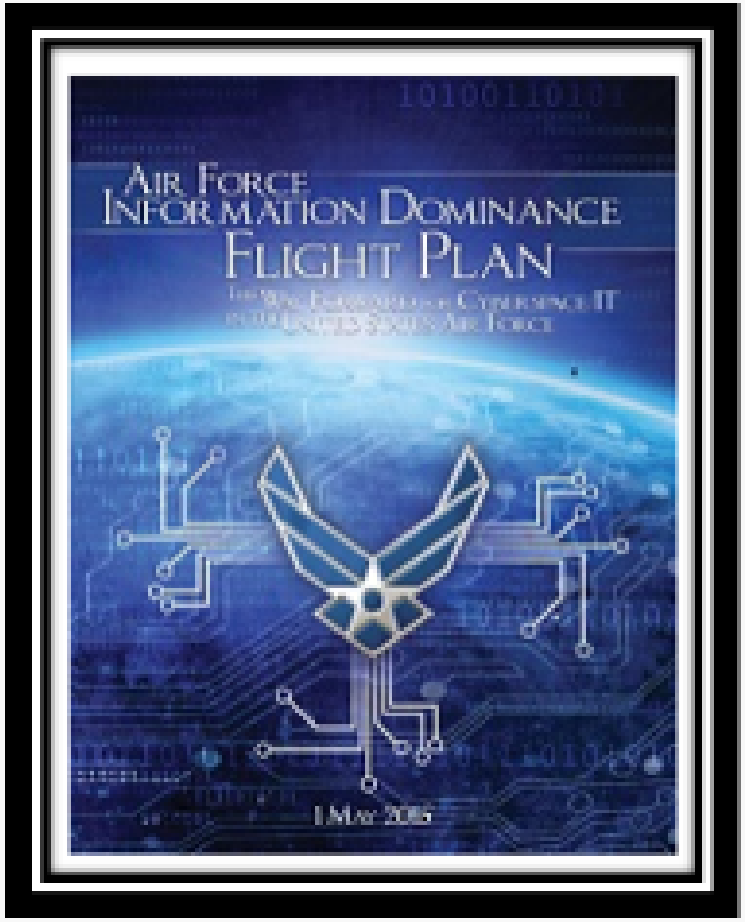
SAF/CIO A6 Mission:
The Chief, Information Dominance and Chief Information Officer (SAF/CIO A6) is the principal advisor to the Secretary of the Air Force, the Chief of Staff of the Air Force, and senior AF leadership on information technology (IT)/Cyberspace and National Security Systems (NSS).

INFORMATION DOMINANCE VISION
The Air Force fully exploits the man-made domain of cyberspace to execute, enhance and support Air Force core missions
PRIORITIZED TENETS (ALWAYS TRUE)
I. Increase Effectiveness of Air Force Core Missions
II. Increase Cybersecurity of Air Force Systems and Information
III. Increase Efficiency Through Innovative IT Solutions
STRATEGIC GOALS (10 YEAR EFFORTS)
1. Provide Airmen trusted information where they need it so they can be most effective
2. Organize, train and educate Cyber-Airmen to become experts in cyberspace and in the Air Force core missions to which they contribute
3. Deliver freedom of action in and through cyberspace to advance Air Force core missions
4. Optimize the planning, programming and execution of cyberspace investments

- **The establishment of the Cyber Mission Forces (CMF) was a US Cyber Command (USCYBERCOM) effort to create a cadre of defenders of the most important "Cyber Key Terrain" (CKT) in cyberspace.**
- **The CKT, defined in the terms of its relationship to a mission or capability, becomes known as an operational mission enclave, leading to the term "enclave defense."**
- **Therefore, Cyber Protection Teams (CPT) provide enclave defense of prioritized missions and focus on only the most important CKT.**
- **Identifying CKT starts with a focus on the supported commander's prioritized mission or capability (not a system, network, or a piece of IT equipment).**
- **The goal of Cyber-Next is to always be ready and not just to prepare for inspections.**

CPTs & MDTs

- CPTs are mobile, responsive, and able to deploy to new prioritized terrain quickly.
- CPT operators already employ a cyberspace weapon system, which is procured, integrated, and sustained by the AF Material Command's AF Lifecycle Management Center (AFLCMC).
- Mission Defense Teams (MDTs) fill in a supply-demand gap for heightened enclave defense capability provided by CPTs.
- The *de facto* activity of MDT operations is their persistent and enduring presence in the network, which reduces the need to reorient to the Cyber Key Terrain.



Unrivaled Global Reach for America … ALWAYS!

Cyber-Next Resources

- The CS-N and MDT initiatives will help maintain an advantage in the cyberspace domain and enable USAF forces the freedom of action necessary to achieve mission objectives.
- Airmen can find additional Cyber-Next information:
  - On the milSuite Comm-Squadron Next Collaboration Site: https://www.milsuite.mil/book/community/spaces/saf-cio-a6/comm-squadron-next
  - On the SAF/CIO A6 SharePoint Site: http[illegible]af.mil[illegible].aspx

milBook
User, team and organization collaboration and networking
Go to milBook
milWiki
Articles on organizations, systems, and places across the DoD
Go to milWiki
milWire
Information sharing service to plug into people and topics
Go to milWire
milTube
Video sharing services where users can upload, watch, and share videos
Go to milTube

References

This brief and additional Information can be found here:

https://eim.amc.af.mil/sites/Cyber/default.aspx

Air Force Instruction 33-200 (31AUG15)
www.e-publishing.af.mil

POC: AMC/A6OS
DSN 779-6298